

CLAIMS

What is claimed is:

1 1. A cryptographic apparatus comprising:
2 a data reading means for reading content data and
3 cryptographic information from a portable storage medium, the
4 cryptographic information including information used to
5 specify a certain part of the content data on which
6 cryptographic processing is to be performed;

7 a part specifying means for specifying, based on the read
8 cryptographic information, the certain part of the read
9 content data; and

10 a cryptographic processing means for performing one of
11 encryption and decryption on the certain part of the read
12 content data.

1 2. The cryptographic apparatus of Claim 1, wherein:

2 a plurality of pieces of content data are each recorded as
3 a file on the storage medium, along with cryptographic
4 information for each of a plurality of file types; and

5 the data reading means reads, from the storage medium, the

6 content data of a file and the cryptographic information for a
7 corresponding file type.

1 3. The cryptographic apparatus of Claim 2, wherein:
2 the cryptographic information includes a reference
3 instruction indicating that a data section in the content data
4 be referred to, and
5 the part specifying means specifies the certain part by
6 referring to the data section as indicated by the reference
7 instruction.

8 4. The cryptographic apparatus of Claim 3, wherein:
9 the cryptographic information includes bit pattern
10 information showing a certain bit sequence; and
11 the part specifying means detects, in the content data, bit
12 data that matches the bit sequence shown in the bit pattern
13 information, and uses a location of the bit data as a basis
14 for specifying the certain part, the certain part having a
15 fixed positional relationship to the bit data.

1 5. The cryptographic apparatus of Claim 4, wherein:
2 the indicated data section shows a length of the certain
3 part; and

4 the part specifying means specifies the certain part of the
5 content data by referring to the data section as indicated by
6 the reference instruction, and calculating the length of the
7 certain part based on the referenced data section.

1 6. The cryptographic apparatus of Claim 5, wherein:
2 the cryptographic information includes a value showing a
3 unit used for the indicated data section; and

4 the part specifying means specifies the certain part by
5 multiplying the length shown by the data section with the unit
6 value to calculate the length of the certain part.

1 7. The cryptographic apparatus of Claim 6, wherein:
2 the cryptographic information further includes a detect
3 instruction for detecting, from the content data, bit data
4 that matches the certain bit sequence shown by the bit pattern
5 information, and determines the order in which the reference
6 and detect instructions are performed; and

7 the part specifying means specifies the certain part in the
8 content data by performing, in the predetermined order,
9 operations indicated by each of the instructions.

1 8. The cryptographic apparatus of Claim 3, wherein:

2 the cryptographic information further includes at least one
3 piece of algorithm information for specifying an algorithm
4 used for cryptographic processing; and

5 the cryptographic processing means performs one of
6 encryption and decryption on the certain part using the
7 specified algorithm.

1 9. The cryptographic apparatus of Claim 2, wherein:

2 the cryptographic information further includes at least one
3 piece of algorithm information for specifying an algorithm
4 used for cryptographic processing; and

5 the cryptographic processing means performs one of
6 encryption and decryption on the certain part using the
7 specified algorithm.

1 10. The cryptographic apparatus of Claim 1, wherein

2 the cryptographic information includes a reference
3 instruction indicating that a data section in the content data
4 be referred to, and

5 the part specifying means specifies the certain part by
6 referring to the data section as indicated by the reference
7 instruction.

1 11. The cryptographic apparatus of Claim 10, wherein:
2 the cryptographic processing means encrypts the certain
3 part; and
4 the cryptographic apparatus further comprises a content
5 data recording means for recording the encrypted content data
6 onto the storage medium.

1 12. The cryptographic apparatus of Claim 10, wherein:
2 the cryptographic processing means decrypts the certain
3 part of the content data; and

4 the cryptographic apparatus further comprises:

5 an encrypting information reading means for reading, from
6 another portable storage medium, encrypting information
7 including information used to specify a certain part in the
8 decrypted content data to be encrypted;

9 an encryption part specifying means for specifying a
10 certain part to be encrypted in the decrypted content data,
11 according to the encrypting information;

12 an encrypting means for encrypting the part specified by
13 the encrypting information; and

14 a content data recording means for recording the encrypted
15 content data onto the other storage medium.

1 13. The cryptographic apparatus of Claim 1, wherein:
2 the cryptographic information further includes at least one
3 piece of algorithm information for specifying an algorithm
4 used for cryptographic processing; and
5 the cryptographic processing means performs one of
6 encryption and decryption on the certain part using the
7 specified algorithm.

1 14. The cryptographic apparatus of Claim 13, wherein:
2 the cryptographic information includes a plurality of
3 pieces of algorithm information, and pieces of range
4 information each showing a range over which an algorithm is
5 applied; and
6 the cryptographic processing means selects, for each
7 application range in the certain part, a piece of algorithm
8 information based on the range information, and uses an
9 algorithm specified by the piece of algorithm information to
10 perform one of encryption and decryption on the application
11 range.

1 15. The cryptographic apparatus of Claim 14, wherein:
2 the cryptographic information includes information showing
3 priority ratings indicating an order in which the pieces of

algorithm information should be applied; and

when the application ranges of a plurality of algorithms overlap, the cryptographic processing means selects pieces of algorithm information according to the priority ratings.

16. The cryptographic apparatus of Claim 1, wherein:

the cryptographic processing means encrypts the certain part; and

the cryptographic apparatus further comprises a content data recording means for recording the encrypted content data onto the storage medium.

17. The cryptographic apparatus of Claim 1, wherein:

the cryptographic processing means decrypts the certain part.

18. The cryptographic apparatus of Claim 17, further comprising:

an encrypting information reading means for reading, from another portable storage medium, encrypting information including information used to specify a certain part in the decrypted content data to be encrypted;

an encryption part specifying means for specifying a

8 certain part to be encrypted in the decrypted content data;
9 according to the encrypting information;
10 an encrypting means for encrypting the part specified by
11 the encrypting information; and
12 a content data recording means for recording the encrypted
13 content data onto the other storage medium.

1 19. A cryptographic apparatus encrypting content data and
2 recording the encrypted data onto a storage medium, the
3 cryptographic apparatus comprising:

4 a content data obtaining means for obtaining content data;

5 a cryptographic information reading means for reading, from
6 a portable storage medium, cryptographic information including
7 information used to specify a certain part of the content data
8 on which cryptographic processing is to be performed;

9 a part specifying means for specifying the certain part of
10 the obtained content data based on the read cryptographic
11 information;

12 a cryptographic processing means for encrypting the certain
13 part; and

14 a content data recording means for recording the encrypted
15 content data onto the storage medium.

1 20. The cryptographic apparatus of Claim 19, wherein:
2 the storage medium stores a plurality of pieces of content
3 data as files, along with cryptographic information for a
4 plurality of file types corresponding to files that can be
5 stored on the storage medium; and
6 the cryptographic information reading means reads the
7 cryptographic information for a file type from the storage
8 medium; and
9 the content data recording means records the encrypted
10 content data onto the storage medium as a file of the file
11 type corresponding to the read cryptographic information.

1 21. The cryptographic apparatus of Claim 20, wherein:
2 the cryptographic information includes bit pattern
3 information showing a certain bit sequence; and
4 the part specifying means detects, in the content data, bit
5 data that matches the bit sequence shown in the bit pattern
6 information, and uses a location of the bit data as a basis
7 for specifying the certain part, the certain part having a
8 fixed positional relationship to the bit data.

1 22. The cryptographic apparatus of Claim 21, wherein:
2 the cryptographic information includes a reference

3 instruction indicating that a data section in the content data
4 be referred to, the data section showing a length of the
5 certain part; and

6 the part specifying means specifies the certain part by
7 referring to the data section as indicated by the reference
8 instruction and calculating the length of the certain part
9 based on the referenced data section.

1 23. The cryptographic apparatus of Claim 21, wherein:

2 the cryptographic information further includes at least one
3 piece of algorithm information specifying an algorithm used
4 for cryptographic processing; and

5 the cryptographic processing means encrypts the certain
6 part using the algorithm specified by the algorithm
7 information.

1 24. The cryptographic apparatus of Claim 19, wherein:

2 the cryptographic information includes bit pattern
3 information showing a certain bit sequence; and

4 the part specifying means detects, in the content data, bit
5 data that matches the bit sequence shown in the bit pattern
6 information, and uses a location of the bit data as a basis
7 for specifying the certain part, the certain part having a

8 fixed positional relationship to the bit data.

9

1 25. The cryptographic apparatus of Claim 24, wherein:
2 the cryptographic information includes a reference
3 instruction indicating that a data section in the content data
4 be referred to, the data section showing a length of the
5 certain part; and

6 the part specifying means specifies the certain part by
7 referring to the data section as indicated by the reference
8 instruction and calculating the length of the certain part
9 based on the referenced data section.

1 26. The cryptographic apparatus of Claim 19, wherein:
2 the cryptographic information further includes at least one
3 piece of algorithm information specifying an algorithm used
4 for cryptographic processing; and

5 the cryptographic processing means encrypts the certain
6 part using the algorithm specified by the algorithm
7 information.

1 27. The cryptographic apparatus of Claim 26, wherein:
2 the cryptographic information includes a plurality of

3 pieces of algorithm information and pieces of range
4 information each showing a range in the content data over
5 which an algorithm is applied; and
6 the cryptographic processing means selects, for each
7 application range in the certain part, a piece of algorithm
8 information based on the range information, and uses an
9 algorithm specified by the piece of algorithm information to
10 encrypt data in the application range.

28. The cryptographic apparatus of Claim 27, wherein:
the cryptographic information includes information showing
priority ratings indicating an order in which the pieces of
algorithm information should be applied; and
when the application ranges of a plurality of algorithms
overlap, the cryptographic processing means selects pieces of
algorithm information according to the priority ratings.

29. A cryptographic apparatus comprising:
a data obtaining means for obtaining, from received data,
content data, and cryptographic information including
information used to specify a certain part of the content data
on which cryptographic processing is to be performed, the
received data consisting of content data and cryptographic

7 information that has been multiplexed and transmitted;
8 a part specifying means for specifying the certain part of
9 the obtained content data based on the obtained cryptographic
10 information; and
11 a cryptographic processing means for performing one of
12 encryption and decryption on the certain part of the content
13 data.

1 30. The cryptographic apparatus of Claim 29, wherein:
2 the cryptographic information includes a reference
3 instruction indicating that a data section in the content data
4 be referred to, and
5 the part specifying means specifies the certain part by
6 referring to the data section as indicated by the reference
7 instruction.

1 31. The cryptographic apparatus of Claim 30, wherein:
2 the cryptographic information includes sync pattern
3 information showing a certain bit sequence; and
4 the part specifying means detects, in the content data, a
5 sync pattern corresponding to the bit sequence shown in the
6 sync pattern information, and uses a location of the sync
7 pattern as a basis for specifying the certain part, the

8 certain part having a fixed positional relationship to the
9 sync pattern.

1 32. The cryptographic apparatus of Claim 31, wherein:

2 the part specifying means verifies the authenticity of the
3 detected sync pattern by checking whether another sync pattern
4 is located at a position a set interval away from the location
5 of the detected sync pattern.

33. The cryptographic apparatus of Claim 31, wherein:

the cryptographic information further includes flag pattern information showing a bit sequence, and position information specifying the position of the bit sequence; and

the part specifying means verifies whether the bit sequence shown by the flag pattern information exists at the position in the content data specified by the position information.

34. The cryptographic apparatus of Claim 31, wherein:

the indicated data section shows a length of the certain
part; and

the part specifying means specifies the certain part of the content data by referring to the data section as indicated by the reference instruction, and calculating the length of the

7 certain part based on the referenced data section.

1 35. The cryptographic apparatus of Claim 34, wherein:
2 the cryptographic information includes a value showing a
3 unit used for the indicated data section; and
4 the part specifying means specifies the certain part by
5 multiplying the length shown by the data section with the unit
6 value to calculate the length of the certain part.

36. The cryptographic apparatus of Claim 35, wherein:
the cryptographic information further includes a detect instruction for detecting, from the content data, bit data that matches the certain bit sequence shown by the bit pattern information, and determines the order in which the reference and detect instructions are performed; and
the part specifying means specifies the certain part in the content data by performing, in the predetermined order, operations indicated by each of the instructions.

1 37. The cryptographic apparatus of Claim 31,
2 the cryptographic information further includes at least one
3 piece of algorithm information for specifying an algorithm
4 used for cryptographic processing; and

5 the cryptographic processing means performs one of
6 encryption and decryption on the certain part using the
7 specified algorithm.

1 38. The cryptographic apparatus of Claim 29, wherein:
2 the cryptographic information further includes at least one
3 piece of algorithm information for specifying an algorithm
4 used for cryptographic processing; and

5 the cryptographic processing means performs one of
6 encryption and decryption on the certain part using the
7 specified

1 39. The cryptographic apparatus of Claim 38, wherein:
2 the cryptographic information includes a plurality of
3 pieces of algorithm information, and pieces of range
4 information each showing a range over which an algorithm is
5 applied; and

6 the cryptographic processing means selects, for each
7 application range in the certain part, a piece of algorithm
8 information based on the range information, and uses an
9 algorithm specified by the piece of algorithm information to
10 perform one of encryption and decryption on the application
11 range.

40. The cryptographic apparatus of Claim 39, wherein:
the cryptographic information includes information showing
priority ratings indicating an order in which the pieces of
algorithm information should be applied; and
when the application ranges of a plurality of algorithms
overlap, the cryptographic processing means selects pieces of
algorithm information according to the priority ratings.

41. The cryptographic apparatus of Claim 29,
the cryptographic processing means decrypts the certain
part.

42. A cryptographic apparatus performing cryptographic processing on content data, the cryptographic apparatus comprising:

- a content data obtaining means for obtaining content data;
- a cryptographic information obtaining means for obtaining cryptographic information including information specifying a part on which cryptographic processing is to be performed in the contents data, the information including a reference instruction indicating that a data section in the content data be referred to;

11 a part specifying means for specifying the certain part of
12 the content data based on the cryptographic information by
13 referring to the data section in the content data as indicated
14 by the reference instruction; and
15 a cryptographic processing means for performing one of
16 encryption and decryption on the certain part.

1 43. The cryptographic apparatus of Claim 42, wherein:
2 the cryptographic information includes bit pattern
3 information showing a certain bit sequence; and
4 the part specifying means detects, in the content data, bit
5 data that matches the bit sequence shown in the bit pattern
6 information, and uses a location of the bit data as a basis
7 for specifying the certain part, the certain part having a
8 fixed positional relationship to the bit data.

1 44. The cryptographic apparatus of Claim 43, wherein:
2 the cryptographic information includes a reference
3 instruction indicating that a data section in the content data
4 be referred to, the data section showing a length of the
5 certain part; and
6 the part specifying means specifies the certain part by
7 referring to the data section as indicated by the reference

8 instruction and calculating the length of the certain part
9 based on the referenced data section.

10

1 45. The cryptographic apparatus of Claim 44, wherein:
2 the cryptographic information includes a value showing a
3 unit used for the indicated data section; and
4 the part specifying means specifies the certain part by
5 multiplying the length shown by the data section with the unit
6 value to calculate the length of the certain part.

7 46. The cryptographic apparatus of Claim 45, wherein:
8 the cryptographic information further includes a detect
9 instruction for detecting, from the content data, bit data
10 that matches the certain bit sequence shown by the bit pattern
11 information, and determines the order in which the reference
12 and detect instructions are performed; and
13 the part specifying means specifies the certain part in the
14 content data by performing, in the predetermined order,
15 operations indicated by each of the instructions.

1 47. The cryptographic apparatus of Claim 42, wherein:
2 the cryptographic information further includes at least one

3 piece of algorithm information for specifying an algorithm
4 used for cryptographic processing; and
5 the cryptographic processing means performs one of
6 encryption and decryption on the certain part using the
7 specified algorithm.

1 48. The cryptographic apparatus of Claim 47, wherein:
2 the cryptographic information includes a plurality of
3 pieces of algorithm information, and pieces of range
4 information each showing a range over which an algorithm is
5 applied; and

6 the cryptographic processing means selects, for each
7 application range in the certain part, a piece of algorithm
8 information based on the range information, and uses an
9 algorithm specified by the piece of algorithm information to
10 perform one of encryption and decryption on the application
11 range.

1 49. The cryptographic apparatus of Claim 48, wherein:
2 the cryptographic information includes information showing
3 priority ratings indicating an order in which the pieces of
4 algorithm information should be applied; and
5 when the application ranges of a plurality of algorithms

6 overlap, the cryptographic processing means selects pieces of
7 algorithm information according to the priority ratings.

1 50. The cryptographic apparatus of Claim 42, wherein:
2 the cryptographic processing means encrypts the certain
3 part of the content data; and
4 the cryptographic apparatus further comprises a
5 multiplexing transmission means for multiplexing the encrypted
6 content data and the cryptographic information and
7 transmitting the multiplexed data.

1 51. A program recording medium storing a control program
2 for having a computer execute cryptographic processing on
3 content data, the control program comprising:

4 a data reading step for reading content data and
5 cryptographic information from a portable storage medium, the
6 cryptographic information including information used to
7 specify a certain part of the content data on which
8 cryptographic processing is to be performed;

9 a part specifying step for specifying, based on the read
10 cryptographic information, the certain part of the read
11 content data; and

12 a cryptographic processing step for performing one of

13 encryption and decryption on the certain part of the read
14 content data.

1 52. The program recording medium of Claim 51, wherein:
2 a plurality of pieces of content data are each recorded as
3 a file on the storage medium, along with cryptographic
4 information for each of a plurality of file types; and
5 the data reading step reads, from the storage medium, the
6 content data of a file and the cryptographic information for a
7 corresponding file type.

1 53. The program recording medium of Claim 51, wherein:
2 the cryptographic information includes bit pattern
3 information showing a certain bit sequence; and
4 the part specifying step detects, in the content data, bit
5 data that matches the bit sequence shown in the bit pattern
6 information, and uses a location of the bit data as a basis
7 for specifying the certain part, the certain part having a
8 fixed positional relationship to the bit data.

1 54. The program recording medium of Claim 51, wherein:
2 the cryptographic information further includes at least one
3 piece of algorithm information for specifying an algorithm

4 used for cryptographic processing; and

5 the cryptographic processing step performs one of

6 encryption and decryption on the certain part using the

7 specified algorithm.

1 55. The program recording medium of Claim 51, wherein:
2 the cryptographic processing step encrypts the certain
3 part; and

4 the cryptographic processing further comprises a content
5 data recording step for recording the encrypted content data
6 onto the storage medium.

56. The program recording medium of Claim 51, wherein:
the cryptographic processing step decrypts the certain
part.

1 57. The program recording medium of Claim 56, wherein the
2 cryptographic processing further comprises:

3 an encrypting information reading step for reading, from
4 another portable storage medium, encrypting information
5 including information used to specify a certain part in the
6 decrypted content data to be encrypted;

7 an encryption part specifying step for specifying a certain

8 part to be encrypted in the decrypted content data, according
9 to the encrypting information;
10 an encrypting step for encrypting the part specified by the
11 encrypting information; and
12 a content data recording step for recording the encrypted
13 content data onto the other storage medium.

1 58. A program recording medium storing a control program
2 for having a computer storing content data execute
3 cryptographic processing on the content data, the
4 cryptographic processing (1) including encryption of the
5 content data and recording of the encrypted content data onto
6 a storage medium, and (2) comprising the following steps:
7 a cryptographic information reading step for reading, from
8 a portable storage medium, cryptographic information including
9 information used to specify a certain part of the content data
10 on which cryptographic processing is to be performed;
11 a part specifying step for specifying the certain part of
12 the obtained content data based on the read cryptographic
13 information;
14 a cryptographic processing step for encrypting the certain
15 part; and
16 a content data recording step for recording the encrypted

17 content data onto the storage medium.

1 59. The program recording medium of Claim 58, wherein
2 the storage medium stores a plurality of pieces of content
3 data as files, along with cryptographic information for a
4 plurality of file types corresponding to files that can be
5 stored on the storage medium; and

6 the cryptographic information reading step reads the
7 cryptographic information for a file type from the storage
8 medium; and

9 the content data recording step records the encrypted
10 content data onto the storage medium as a file of the file
11 type corresponding to the read cryptographic information.

12 60. The program recording medium of Claim 58, wherein:

13 the cryptographic information includes bit pattern
14 information showing a certain bit sequence; and

15 the part specifying step detects, in the content data, bit
16 data that matches the bit sequence shown in the bit pattern
17 information, and uses a location of the bit data as a basis
18 for specifying the certain part, the certain part having a
19 fixed positional relationship to the bit data.

1 61. The program recording medium of Claim 58, wherein:
2 the cryptographic information further includes at least one
3 piece of algorithm information for specifying an algorithm
4 used for cryptographic processing; and
5 the cryptographic processing step performs encryption on
6 the certain part using the specified algorithm.

1 62. A program recording medium storing a control program
2 for having a computer execute cryptographic processing on
3 content data, the cryptographic processing comprising:
4 a data obtaining step for obtaining, from received data,
5 content data, and cryptographic information including
6 information used to specify a certain part of the content data
7 on which cryptographic processing is to be performed, the
8 received data consisting of content data and cryptographic
9 information that has been multiplexed and transmitted;
10 a part specifying step for specifying the certain part of
11 the obtained content data based on the obtained cryptographic
12 information; and
13 a cryptographic processing step for performing one of
14 encryption and decryption on the certain part of the content
15 data.

1 66. A program recording medium storing a control program
2 for having a computer execute cryptographic processing on
3 content data, the cryptographic processing comprising:
4 a content data obtaining step for obtaining content data;
5 a cryptographic information obtaining step for obtaining
6 cryptographic information including information specifying a
7 part on which cryptographic processing is to be performed in
8 the contents data, the information including a reference
9 instruction indicating that a data section in the content data
10 be referred to;
11 a part specifying step for specifying the certain part of
12 the content data based on the cryptographic information by
13 referring to the data section in the content data as indicated
14 by the reference instruction; and
15 a cryptographic processing step for performing one of
16 encryption and decryption on the certain part.

1 67. The program recording medium of Claim 66, wherein:
2 the cryptographic information includes bit pattern
3 information showing a certain bit sequence; and
4 the part specifying step detects, in the content data, bit
5 data that matches the bit sequence shown in the bit pattern

6 information, and uses a location of the bit data as a basis
7 for specifying the certain part, the certain part having a
8 fixed positional relationship to the bit data.

1 68. The program recording medium of Claim 67, wherein:
2 the indicated data section shows a length of the certain
3 part; and

4 the part specifying step specifies the certain part of the
5 content data by referring to the data section as indicated by
6 the reference instruction, and calculating the length of the
7 certain part based on the referenced data section.

1 69. The program recording medium of Claim 66, wherein:
2 the cryptographic information further includes at least one
3 piece of algorithm information for specifying an algorithm
4 used for cryptographic processing; and

5 the cryptographic processing step performs one of
6 encryption and decryption on the certain part using the
7 specified algorithm.

1 70. A portable data recording medium storing encrypted
2 content data, the data recording medium comprising:

3 a content data recording area in which content data, of

4 which a certain part has been encrypted, is recorded; and
5 a cryptographic information recording area in which
6 cryptographic information, including information used to
7 specify the certain part of the content data, is recorded.

1 71. The data recording medium of Claim 70, wherein:
2 each of a plurality of pieces of encrypted content data is
3 recorded as a file in the content data recording area; and
4 cryptographic information is recorded in the cryptographic
5 information recording area according to file type.

6 72. The data recording medium of Claim 71, wherein:
7 the cryptographic information includes a reference
8 instruction instructing a decrypting apparatus decrypting the
9 content data to refer to a data section in the content data.

1 73. The data recording medium of Claim 72, wherein:
2 the cryptographic information includes bit pattern
3 information showing a certain bit sequence, and information
4 instructing the decrypting apparatus to detect, in the content
5 data, bit data matching the certain bit sequence and use a
6 location of the bit data as a basis for specifying the certain
7 part, the certain part having a fixed positional relationship

3 instruction for detecting, from the content data, bit data
4 that matches the certain bit sequence shown by the bit pattern
5 information, and the decryption apparatus determines the order
6 in which the reference and detect instructions are performed.

1 78. The data recording medium of Claim 70, wherein:
2 the cryptographic information further includes at least one
3 piece of algorithm information specifying an algorithm to be
4 used when decrypting the content data.

1 79. The data recording medium of Claim 78, wherein:
2 the cryptographic information includes a plurality of
3 pieces of algorithm information and pieces of range
4 information showing the application range of each piece of
5 algorithm information.

1 80. The data recording medium of Claim 79, wherein:
2 the cryptographic information includes priority ratings
3 used to determine which algorithm information should be
4 applied when the application ranges of a plurality of pieces
5 of algorithm information overlap.

1 81. A cryptographic processing method, comprising:

2 a data reading step for reading content data and
3 cryptographic information from a portable storage medium, the
4 cryptographic information including information used to
5 specify a certain part of the content data on which
6 cryptographic processing is to be performed;

7 a part specifying step for specifying, based on the read
8 cryptographic information, the certain part of the read
9 content data; and

10 a cryptographic processing step for performing one of
11 encryption and decryption on the certain part of the read
12 content data.

1 82. A cryptographic processing method encrypting content
2 data and recording the encrypted content data onto a storage
3 medium, the cryptographic processing method comprising:

4 a cryptographic information reading step for reading, from
5 a portable storage medium, cryptographic information including
6 information used to specify a certain part of the content data
7 on which cryptographic processing is to be performed;

8 a part specifying step for specifying the certain part of
9 the obtained content data based on the read cryptographic
10 information;

11 a cryptographic processing step for encrypting the certain

12 part; and

13 a content data recording step for recording the encrypted
14 content data onto the storage medium.

1 83. A cryptographic processing method performing
2 cryptographic processing on content data, the cryptographic
3 method comprising:

4 a data obtaining step for obtaining, from received data,
5 content data, and cryptographic information including
6 information used to specify a certain part of the content data
7 on which cryptographic processing is to be performed, the
8 received data consisting of content data and cryptographic
9 information that has been multiplexed and transmitted;

10 a part specifying step for specifying the certain part of
11 the obtained content data based on the obtained cryptographic
12 information; and

13 a cryptographic processing step for performing one of
14 encryption and decryption on the certain part of the content
15 data.

1 84. A cryptographic processing method performing
2 cryptographic processing on content data, the cryptographic
3 processing method comprising:

4 a content data obtaining step for obtaining content data;
5 a cryptographic information obtaining step for obtaining
6 cryptographic information including information specifying a
7 part on which cryptographic processing is to be performed in
8 the contents data, the information including a reference
9 instruction indicating that a data section in the content data
10 be referred to;

11 a part specifying step for specifying the certain part of
12 the content data based on the cryptographic information by
13 referring to the data section in the content data as indicated
14 by the reference instruction; and

15 a cryptographic processing step for performing one of
16 encryption and decryption on the certain part.